IT Portfolio

Deonte Wynn

Version 1
2022

A message from Deonte` Wynn

You can download my resume along with my IT Portfolio in a PDF document. This portfolio list all individual projects, experiences, community service, references, and articles I've contributed to information technology.

INTRODUCTION

My name is Deonte Wynn. I've been working in IT for 2.5 years. I have always been good with computers since the age of 7. I love learning new information and networking with new professionals. Domains such as Cybersecurity, Networking, and Ethical Hacking, excite me and drive me to become a better professional each day.

I am results driven and my work ethic speaks for it's self. Please take a look at my work, and if you have any questions, my contact information is at the beginning and end.

Thank you and welcome to my Portfolio.

WHAT DISTINGUISHES ME FROM THE PACK?

Aside from having some years in IT as a technical analyst. I've also served in the counseling profession as a therapist. My past experiences required skills such as customer service, conflict resolution, psyche evaluations, and peer-to-peer mediation.

This gives me an advantage when it comes to understanding the motives of people such as "the bad guys" and how to diffuse risky situations. I've also taught and tutored more than 150 students during my time as a College Ed counselor and as an active CompTIA tutor. Having these various faculties has helped me make a smooth transition it into the IT field. I've used these skills to work with hundreds of people and to mitigate computer systems.

Contact Information

Email:
dwynn93@gmail.com

Number:
(484)-343-6010

LinkedIN:
Deonte` Wynn

Credentials & Licenses

CompTIA Security+
CompTIA Network+
CompTIA CIOS (Stackable Certification)
CompTIA CSIS (Stackable Certification)
Dell DSCE (Dell Certified System Expert)
CompTIA A+

Soft Skills

- Research
- Commitment to Learning
- Verbal
- Written Communication
- Leadership
- Networking
- Problem-solving
- Attention to detail
- Composure

Hard Skills

- Computer Networking
- Implementation
- Malware analysis
- Vulnerability assessments
- Risk Analysis
- Security Analysis
- Intrusion Detection/Prevention

EXPERIENCE AND PROJECT DEMOS

The following are all demonstrations of knowledge based on my personal experience, studies and projects.

CYBERSECURITY EXPERIENCE

The following are all cybersecurity experiences i've have done personally or guided by a certified InfoSec Analyst during my current shadowing experience.

INCIDENT RESPONSE AND VIRUS MITGATION WITH SENTINELONE.

In this demonstration I will walk you through an instance with SentinelOne Endpoint Security Platform.

VIRUS MITIGATION AND INVESTIGATION.

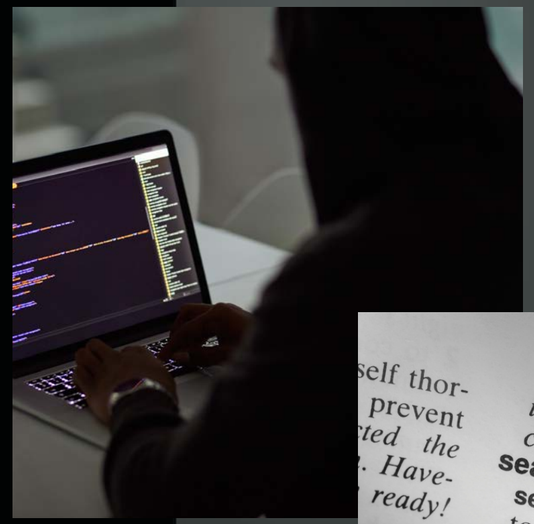
In this particular incident, the end-user mistakenly clicked on a malicious site that was pretending to be Walmart. It redirected the user to a malicious URL/IP address. The first remediation step I did was take the computer off the network via SentinelOne.

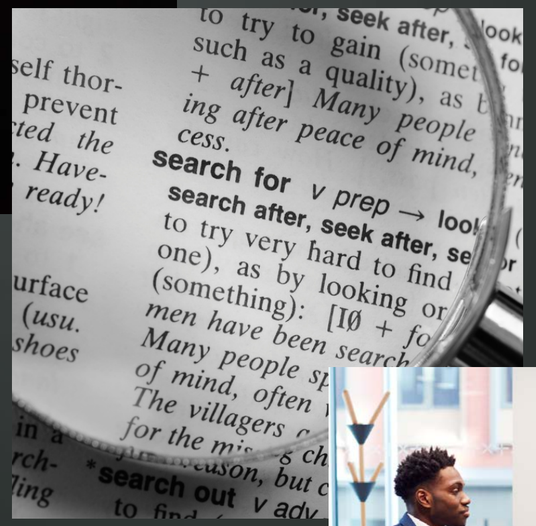
I scheduled a meeting with the end-user to gain information about the malicious site to see if they had knowledge about it.

I looked at the end-user browser history and found the malicious site.

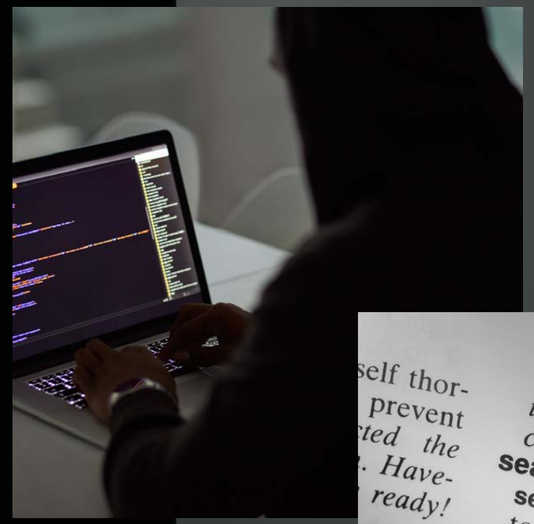
The Information security analyst and myself looked in the settings of the end User's Google Chrome browser.

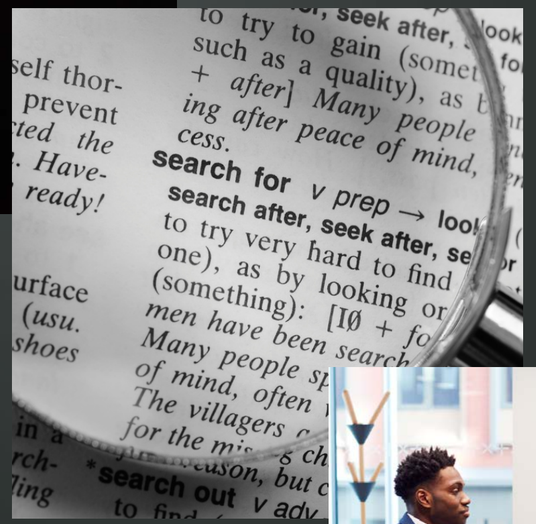
I made sure that security, bookmarks and search engines were standard and not altered.





VIRUS MITIGATION AND INVESTIGATION.





Once we confirmed that the virus was from the malicious URL I took a few steps of securing the system by:

- Checking for any malicious software on the PC.
- Running an A/V scan via SentinelOne and confirming no other viruses were present on the machine.
- Checking networking IPv4 Settings and Proxy Settings.
- Deleted malicious URL.
- Rescaned the PC for safety and enabled network capability.

After the machine was cleared and clean of viruses, I spoke to the end-user on best practices on keeping their machine safe and to look out for potentially unwanted programs/viruses.

REPORTING AND CORRESPONDENCE

Here are my findings below:

Step 1: Ran a scan using S1. Nothing malicious was found on the system.
Step 2: I've opened the task manager to search for any malicious processes that are still open on the system. I did not see anything suspicious.
Step 3: I've ran sfc /scannow in the cmd.
Step 4: Review of Google Chrome settings. All settings are standard.
Step 5: Review of Google Chrome extensions. All extensions look approved from the Chrome Store.
Step 6: I used the command prompt to run the following C:\>attrib -r -a -s -h *.* to detect any executables. I did not see anything at all

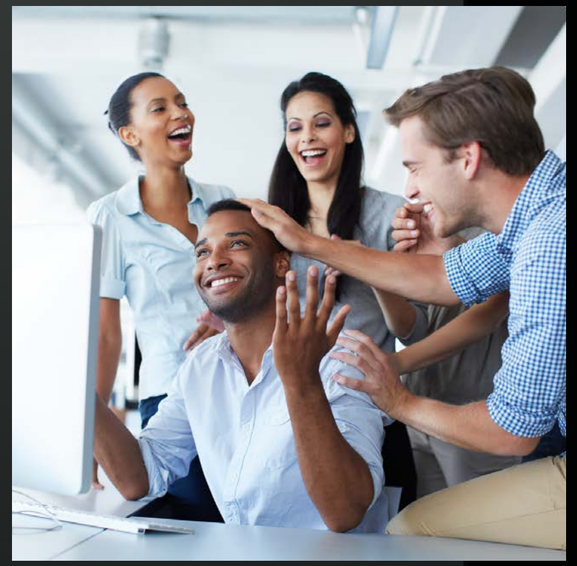
PATCHING VULNERABILITIES AND THREAT HUNTING WITH SENTINELONE.

In this demonstration I will walk you through an instance with SentinelOne Endpoint Security Platform.

THREAT HUNTING AND PATCHING.

During this instance, company XYZ was managing Tyco CCURE and through the SentinelOne Platform I discovered a potential threat that needed to be mitigated with a patch. The patch helped with a vulnerability released from Tyco. Here are the following steps I took to safeguard the systems.

- I downloaded the newest Service Pack from the service providers remote server.
- I took that new Service Pack and uploaded it on a flash drive.
- I spoke to the respective departments and coordinated appropriate times to install the Service Packs on the systems and machines.
- Once the Service Packs were installed I verified for successful installation and full functionality.



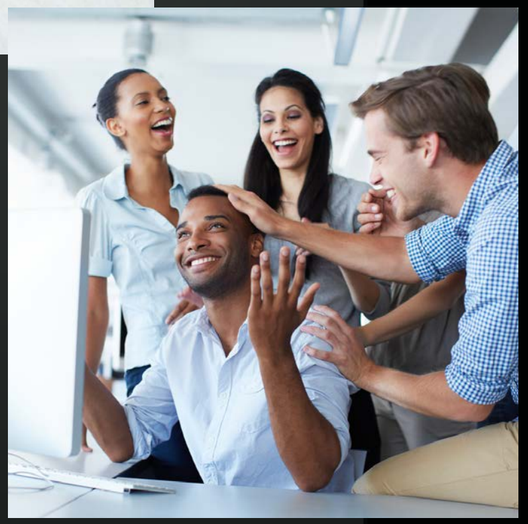
SOFTWARE SECURITY ASSESMENTS WITH SENTINELONE.

In this demonstration I will walk you through an instance with SentinelOne Endpoint Security Platform.

THREAT HUNTING AND PATCHING.

During this instance, company XYZ primarily used SentinelOne and Kace Management for system management and security. We were having issues with other conflicting anti-virus software. This A/V software on these machines needed to go. The following procedures were used to mitigate the potential threat to the network.

- First I identified the machines that contained the conflicting A/V software using SentinelOne.
- I correctly identified the version of the executable programs and searched for the uninstall strings or msi.exe on the A/V websites.
- Using the device management software I could use the uninstall strings to uninstall the A/V software on the devices whenever user logged in.
- I needed to run a silent install so that we would not interrupt users.
- After that, I verified full functionality and confirmed with security analyst.



```
msiexec /x {CE15D1B6-19B6-4D4D-8F43-CF5D2C3356FF} REMOVE=ALL REBOOT=R /q

CylanceProtect_x64.msi /quiet /norestart /uninstall /X{2E64FC5C-9286-4A31-916B-0D8AE4B22954}

C:\Program Files\Malwarebytes\Anti-Malware\mbuns.exe" /Uninstall /uselocalisvc MB
```

```
msiexec /x {2E64FC5C-9286-4A31-916B-0D8AE4B22954}

msiexec /q /x eeff64.msi
```

```
MsiExec.exe /X{3D8647AD-0583-4548-A3A7-4702E625EABB}

C:\ProgramData\Package Cache\{1706e61a-227e-4107-8d01-24431f9c5143}\McAfeeSafeConnect.exe" /uninstall

MsiExec.exe /X{CD426109-9B3A-47E1-AFF8-9EC9F15D36B9}

MsiExec.exe /X{F210DAEC-9E43-467E-87E8-B02DA469CFFC}

C:\ProgramData\Package Cache\{095c98d4-cc8d-4a11-9c82-9ed357ac4f7f}\McAfeeSafeConnect.exe" /uninstall

MsiExec.exe /X{1B96C0AE-247D-469F-BDC7-B3FA11AD383A}

C:\ProgramData\Package Cache\{2973b354-fb68-4cf9-a20a-5bf99895504b}\McAfeeSafeConnect.exe" /uninstall

C:\ProgramData\Package Cache\{783594dd-d2ad-49ea-90a5-b2595c064a19}\McAfeeSafeConnect.exe" /uninstall

MsiExec.exe /X{40204117-C6EB-4719-8726-7F2C0963B574}

C:\Program Files (x86)\McAfee Security Scan\uninstall.exe"

C:\Program Files\McAfee\WebAdvisor\Uninstaller.exe

C:\Program Files\McAfee\WebAdvisor\Uninstaller.exe
```

Software Detail: Cylance PROTECT - Dell Plugins

Created: [redacted]

Modified: [redacted]

Name: (required)
Cylance PROTECT - Dell Plugins

README File Location:

Publisher Information Link:
http://cylance.com

Version:
2.0.1461.32

Publisher:
Cylance, Inc.

Information Link:
http://cylance.com

Assign To Label:
Manage Associated Labels

Uninstall Command:

```
MsiExec.exe /X{49C9F0C5-FCC3-4E5B-A2FA-FCFD0B1CEF30}
```

Notes:

Supported Operating Systems:
All
Manage Operating Systems

Upload and Associate File:
Choose File No file chosen

Don't Replicate Associated File

SECURING AND DECOMMISSIONING LEGACY SYSTEMS WITH SENTINELONE.

In this demonstration I will walk you through an instance with SentinelOne Endpoint Security Platform.

ANALYZING AND DEPROVISIONING

During this instance, company XYZ still had a few systems that had Windows 7 installed on them which was a major security risk to the network. The next steps included:

- Finding and identifying systems that had Windows 7 Software on them.
- Taking those machines and disabling them via SentinelOne or physically removing them from the network.
- Reimaging the machines to a fresher Windows 10 Image.
- After the process we recorded each device in the asset tag inventory and reconnected to the SentenelOne Endpoint Platform for secure monitoring.

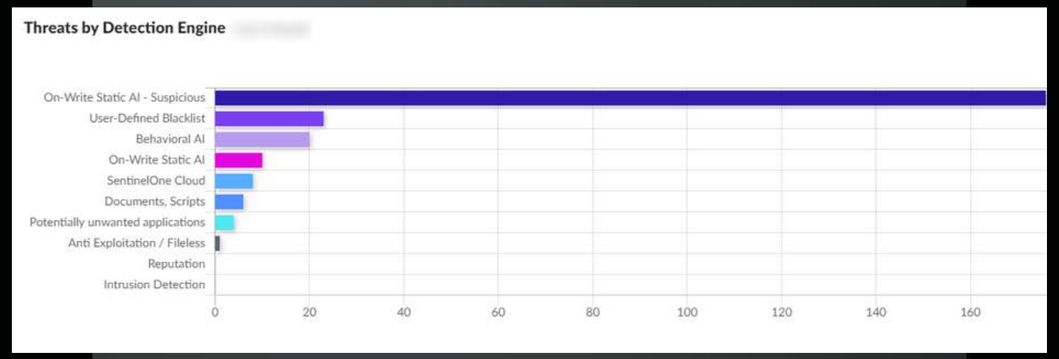
SECURING AND REINSTALLATION OF DECOMMISSIONED DEVICES WITH SENTINELONE.

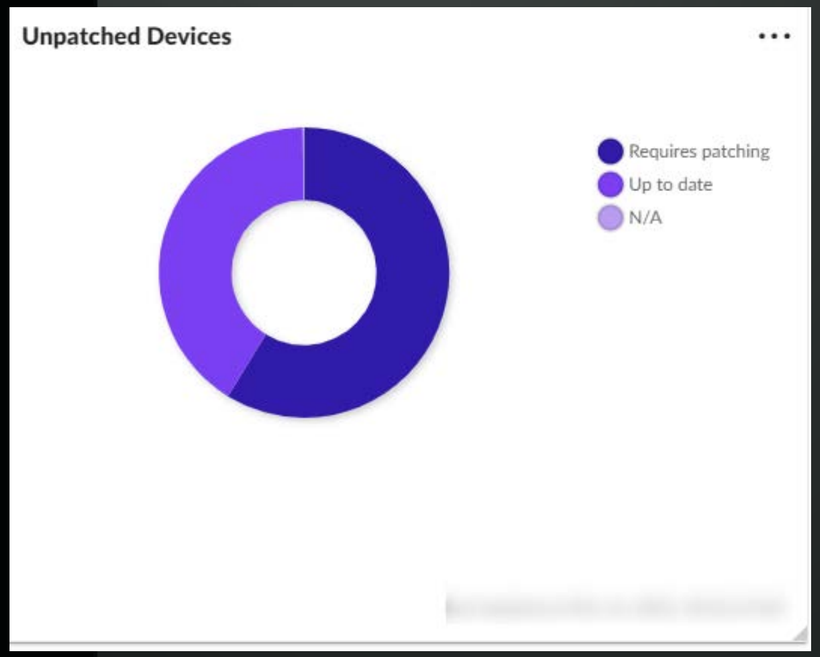
In this demonstration I will walk you through an instance with SentinelOne Endpoint Security Platform.

SECURING FLAGARANT DEVICES

During this instance, I needed to reinstall and rename endpoints in our security platform. This task required me to reach out to the proper departments and facilitate remote sessions and in-person sessions. Figure 1B shows all unpatched devices. You can see the ratio of Up-to-date and unpatched. I used this information to see how I needed to plan and structure my approach to troubleshooting these devices.

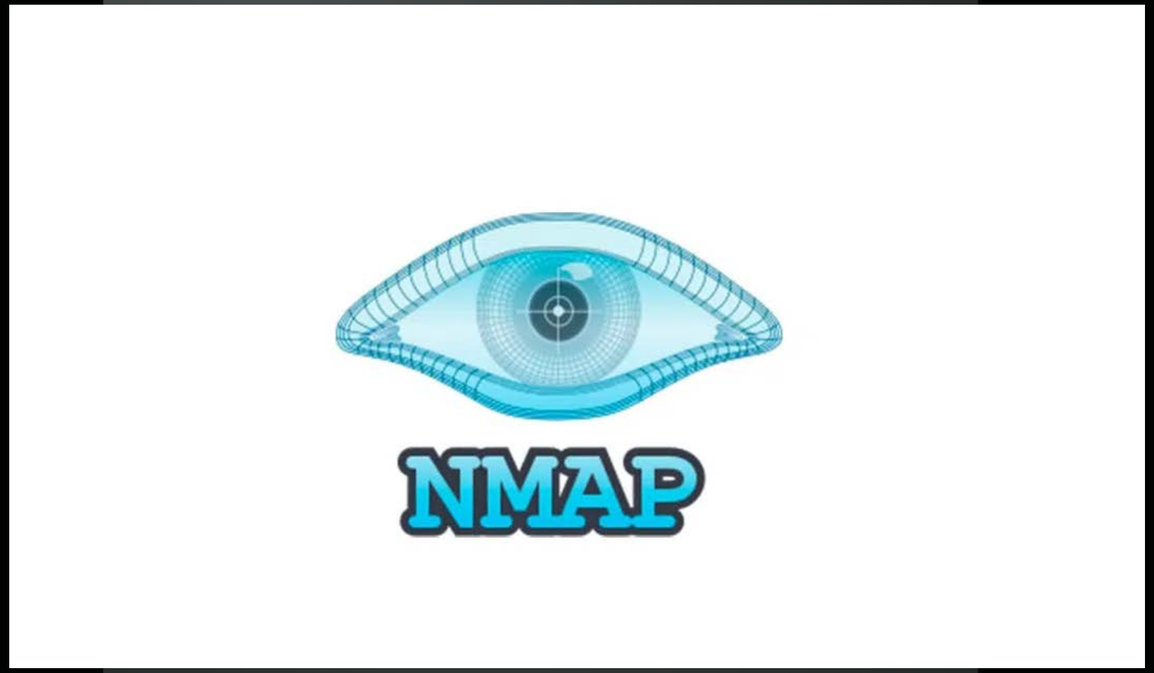
- Established a session with the end-user and configured the endpoint to prepare for installation of SentinelOne on machine.
- After the device is connected to the security endpoint platform scans are ran on the device and confirmed patched and secure.
- These devices were also recorded in companies asset tag database and renamed to companies domain.





RUNNING VULNERABILITY SCANS WITH NMAP

In this demonstration I will walk you through an instance with running vulnerability scans using tools like Nmap and sn1per on Kali Linux

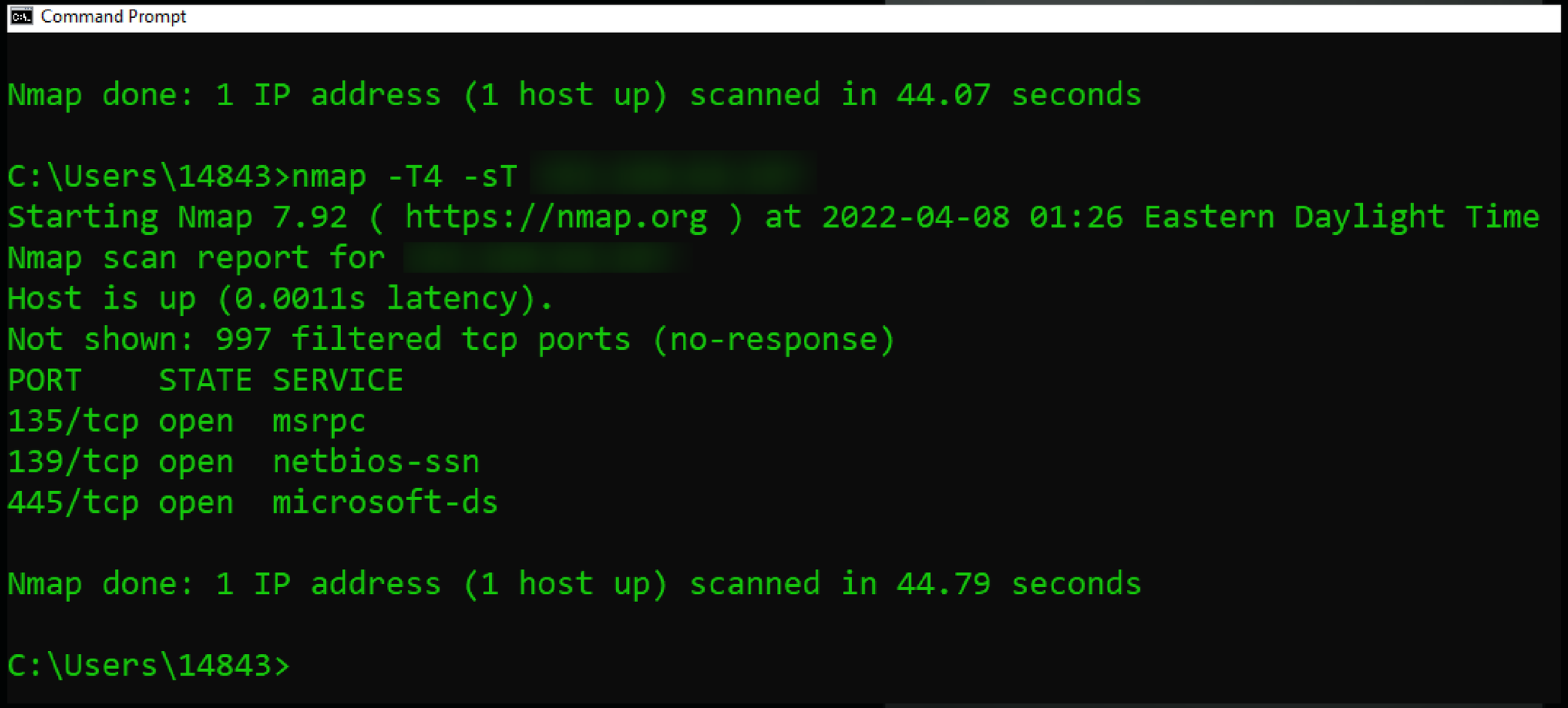


VULNERABILITY SCANS FOR BUSINESS DOMAIN

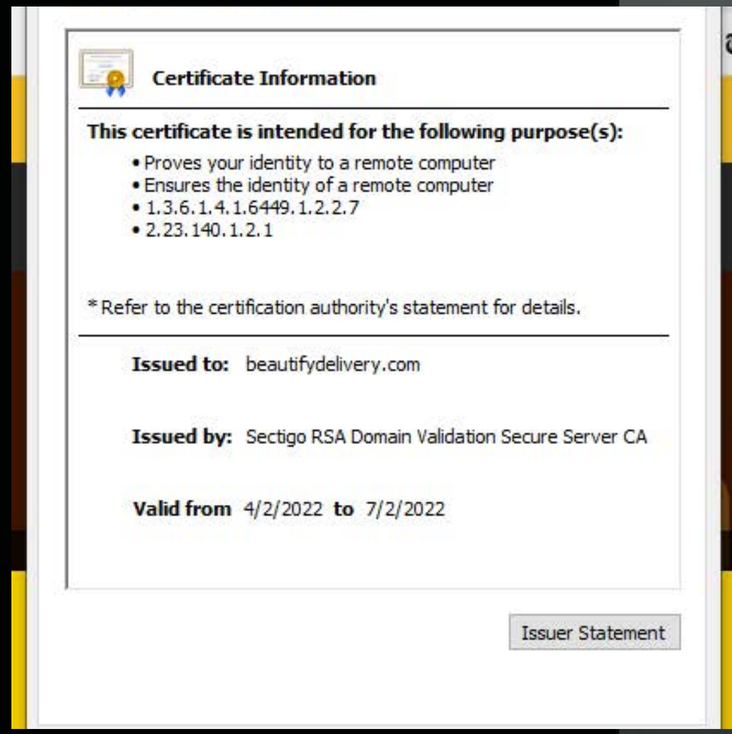
In this demonstration I will walk you through how I run some vulnerability scans for Beautify Delivery. A beauty supplies delivery company. The goal was to make sure that their webserver and url had the proper safe gaurds to thwart possible malicious intent and to see if they had any holes in their defense.

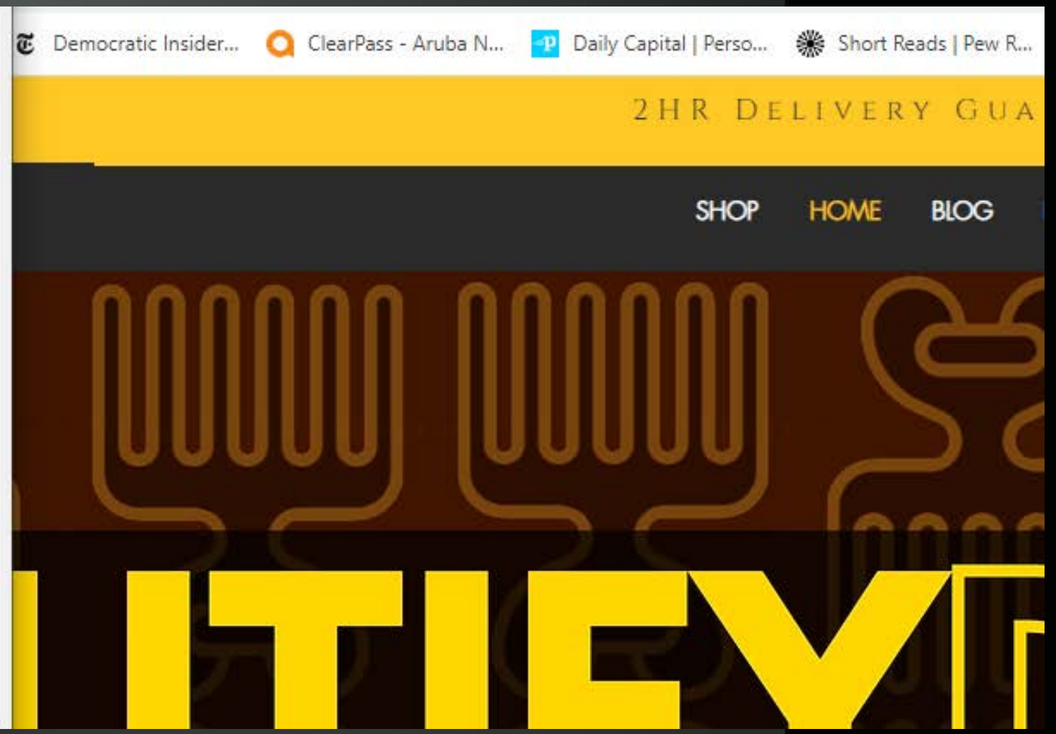
RUNNING VULNERABILITY SCANS WITH NMAP

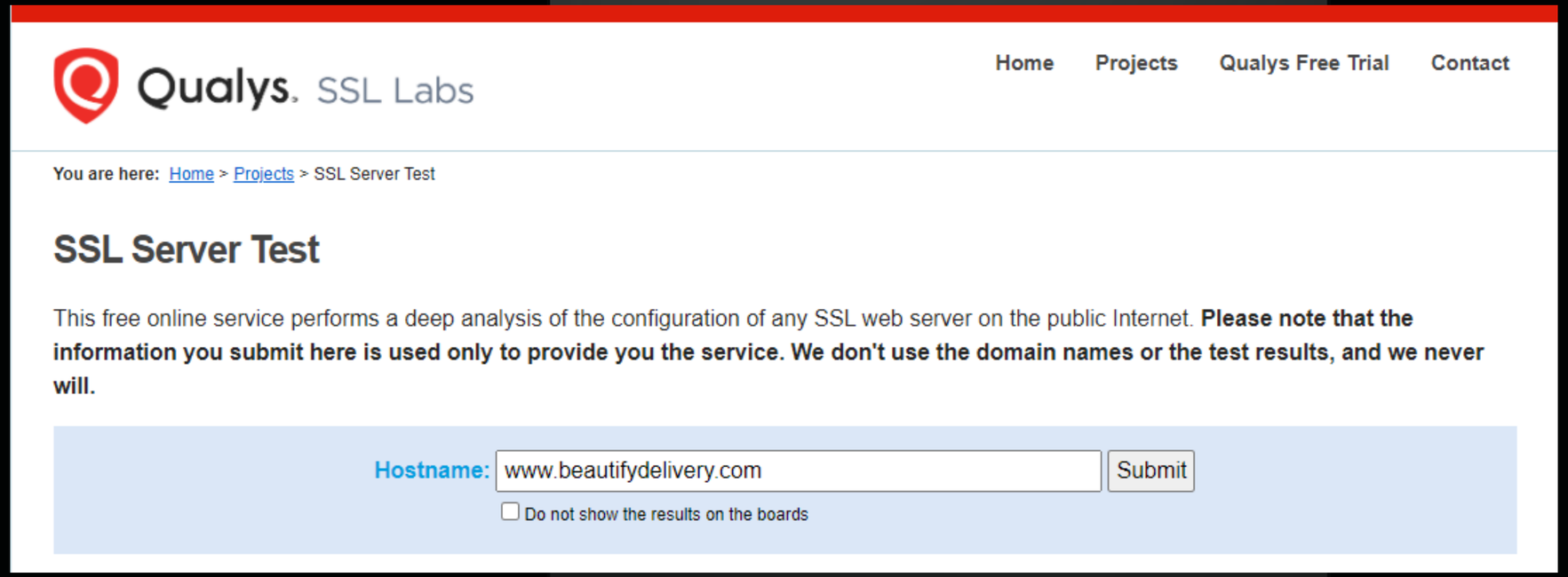
Here I display a common nmap scan targeting tcp ports with T4 for a quick processing speed template. Other scans include Nessus scans and sn1per scans on Kali Linux to enumerate target IP's



For Beautify Delivery I looked at the website's digital certificate to make sure it was up to date. I was able to verify the encryption standard and the issuer statement. The next step I did was cross-checking the SSL configuration with Qualys. The results came back good. The certificate, embedded protocol, key exchange, and cipher strength are configured securely. The next steps will be to run a simple vulnerability scan to see if any holes exist on the webserver.



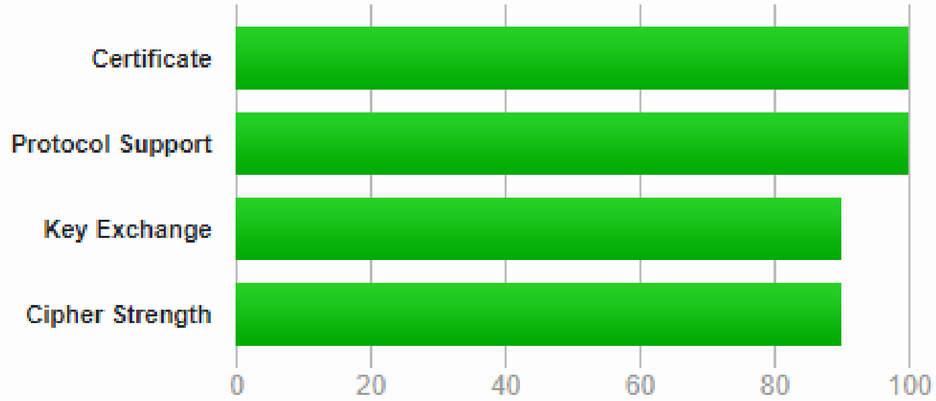




Summary

Overall Rating

A



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This site works only in browsers with SNI support.

This server supports TLS 1.3.

I've run Nmap using a few parameters to get some information that was needed such as DNS info, and OS in use. Since I know that it's a webserver I just needed to see if any ports were vulnerable. In the other figure, I used nslookup just to get the IP address of the domain name. I decided to use sn1per on my Kali Linux virtual machine to do some in-depth reconnaisance.

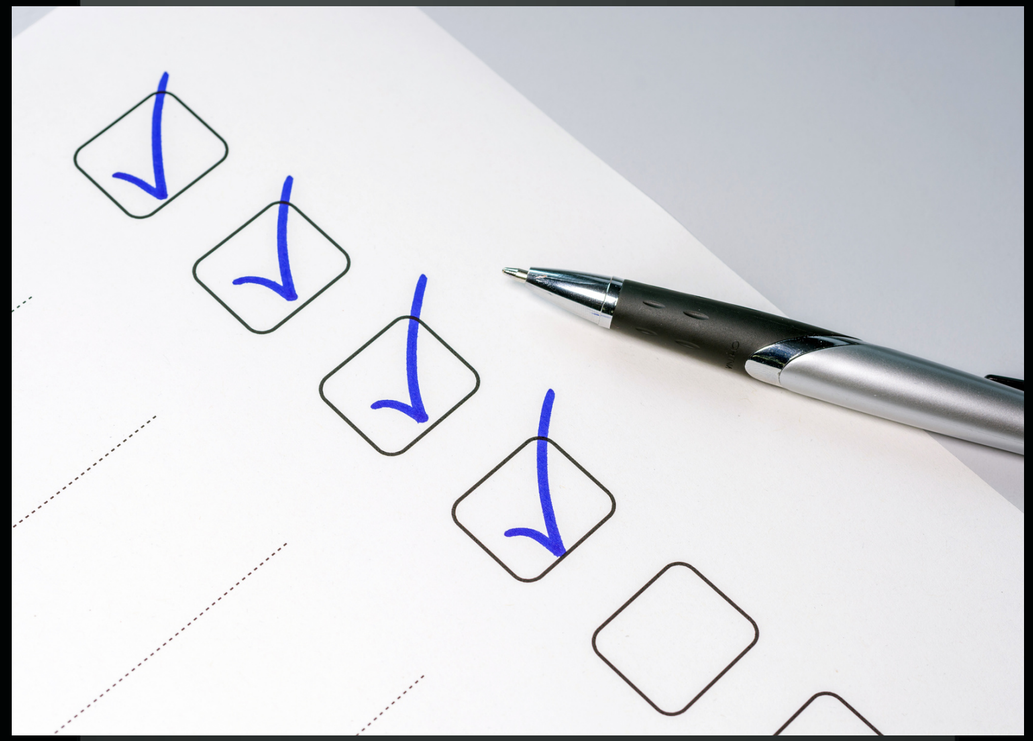
```
Non-authoritative answer:
Name:    td-ccm-168-233.wixdns.net
Address:
Aliases:  www.beautifydelivery.com
          gcdn0.wixdns.net
```

```
nmap -T4 -A -v -Pn
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-08 15:14 Eastern Daylight Time
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:14
Completed NSE at 15:14, 0.00s elapsed
Initiating NSE at 15:14
Completed NSE at 15:14, 0.00s elapsed
Initiating NSE at 15:14
Completed NSE at 15:14, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 15:14
Completed Parallel DNS resolution of 1 host. at 15:14, 0.04s elapsed
Initiating SYN Stealth Scan at 15:14
Scanning 233.168.117.34.bc.googleusercontent.com ( ) [1000 ports]
SYN Stealth Scan Timing: About 29.55% done; ETC: 15:16 (0:01:14 remaining)
SYN Stealth Scan Timing: About 59.55% done; ETC: 15:16 (0:00:41 remaining)
Completed SYN Stealth Scan at 15:16, 101.56s elapsed (1000 total ports)
Initiating Service scan at 15:16
Initiating OS detection (try #1) against 233.168.117.34.bc.googleusercontent.com ( )
Retrying OS detection (try #2) against 233.168.117.34.bc.googleusercontent.com ( )
Initiating Traceroute at 15:16
Completed Traceroute at 15:16, 9.07s elapsed
NSE: Script scanning .
Initiating NSE at 15:16
Completed NSE at 15:16, 0.00s elapsed
Initiating NSE at 15:16
Completed NSE at 15:16, 0.00s elapsed
Initiating NSE at 15:16
Completed NSE at 15:16, 0.00s elapsed
Nmap scan report for 233.168.117.34.bc.googleusercontent.com ( )
Host is up.
All 1000 scanned ports on 233.168.117.34.bc.googleusercontent.com ( ) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details

TRACEROUTE (using proto 1/icmp)
HOP RTT     ADDRESS
1   ... 30

NSE: Script Post-scanning.
Initiating NSE at 15:16
Completed NSE at 15:16, 0.00s elapsed
Initiating NSE at 15:16
Completed NSE at 15:16, 0.00s elapsed
Initiating NSE at 15:16
Completed NSE at 15:16, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 118.31 seconds
           Raw packets sent: 2138 (97.192KB) | Rcvd: 180 (15.693KB)
```

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo sniper beautifydelivery.com
[sudo] password for
 + -- --=[Sniper <html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>openresty</center>
</body>
 is available to download... Do you want to update? (y or n)
n

 + -- --=[http://crowdshield.com
 + -- --=[sniper v2.5a by 1N3

 + -- ----------=[Running Nslookup]=---------- -- +
Server:
Address:

Non-authoritative answer:
Name:   beautifydelivery.com
Address:
Name:   beautifydelivery.com
Address:
Name:   beautifydelivery.com
Address:

beautifydelivery.com has address
beautifydelivery.com has address
beautifydelivery.com has address
beautifydelivery.com mail is handled by 20 alt1.aspmx.l.google.com.
beautifydelivery.com mail is handled by 50 alt4.aspmx.l.google.com.
beautifydelivery.com mail is handled by 10 aspmx.l.google.com.
beautifydelivery.com mail is handled by 30 alt2.aspmx.l.google.com.
beautifydelivery.com mail is handled by 40 alt3.aspmx.l.google.com.
 + -- ----------=[Checking OS Fingerprint]=---------- -- +
/usr/bin/sniper: line 718: xprobe2: command not found
 + -- ----------=[Gathering Whois Info]=---------- -- +
   Domain Name: BEAUTIFYDELIVERY.COM
   Registry Domain ID: 2529550703_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.google.com
   Registrar URL: http://domains.google.com
```

```
+ -- ----------=[Running Web Vulnerability Scan]=---------- -- +
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          [redacted]
+ Target Hostname:    beautifydelivery.com
+ Target Port:        80
+ Message:           Multiple IP addresses found: [redacted]
+ Start Time:        2022-04-09 11:50:26 (GMT-4)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-wix-request-id' found, with contents: 1649519425.68612223173904131634
+ Uncommon header 'server-timing' found, with contents: cache;desc=hit, varnish;desc=hit, dc;desc=42
+ Uncommon header 'x-seen-by' found, with contents: jeslxIFvDH4ulYwNNi+3Muwfbs+7qUVAqsIx00yI78k=,sHU62EDOGnH2FBkJkG/Wx8EeXWsWdHrhlvbxtlynkVhc
w1HIzZ,m0j2EEknGIVUW/liY8BLLlPVSO1QPQ7KlY+JzrfjmCIMbwluI1yUDJty9McxOlfY,2d58ifebGbosy5xc+FRaloHPrPXdh9eTqbw5ByEIH1jQz4n2i0YsIlMRJtVR5rVrH6y5a
DAA==,2UNV7KOq4oGjA5+PKsX47Cbe/tT3rmjvdOcTIXYlFyYfbJaKSXYQ/lskq2jK6SGP
+ Root page / redirects to: https://www.beautifydelivery.com/
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated:  20 error(s) and 5 item(s) reported on remote host
+ End Time:          2022-04-09 11:50:35 (GMT-4) (9 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

CYBERSECURITY DOCUMENTATION AND ILLUSTRATION.

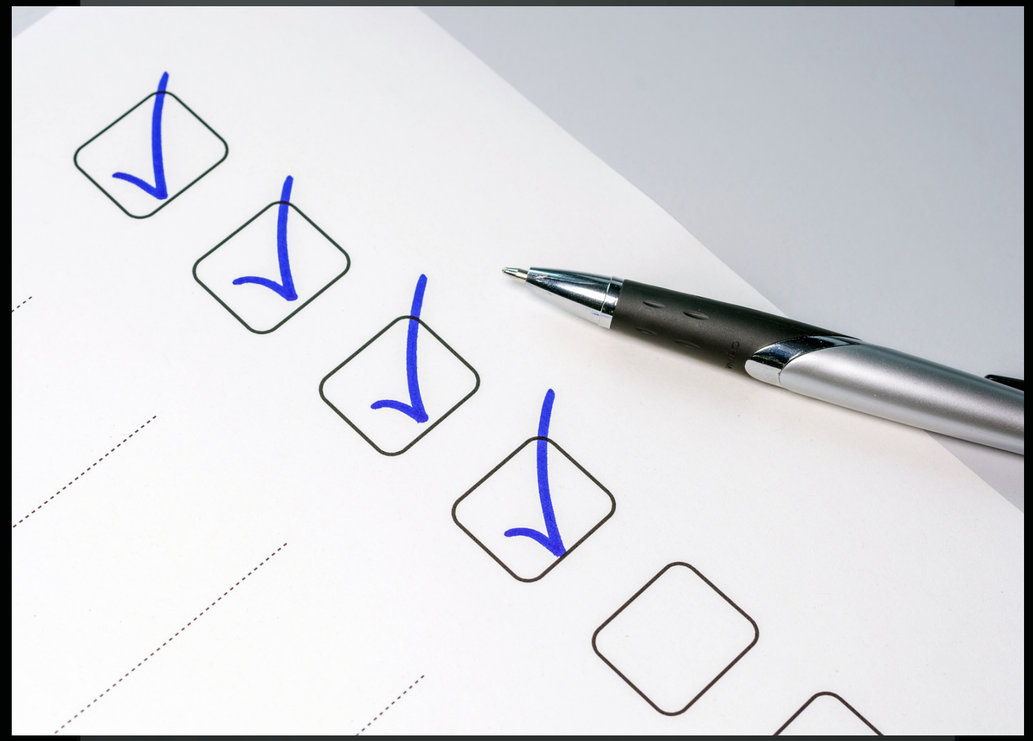


It's imperative that our children and teenagers are safe and sound on the Internet. Our young people need the proper information to help avoid any unwanted #data and #privacy breaches. In this document, I've created a simple guide on how children and teens can be safe on the internet. If you're a parent, guardian, or a good samaritan it's important that you share this with your family and friends. Being #cybersafe starts with us as a community.

CYBERSAFE DOCUMENTATION AND ILLUSTRATION

CYBERSECURITY DOCUMENTATION AND ILLUSTRATION.

In this example, here I walk you through an instance where I use my knowledge of NIST 800-53 and ISO to construct a simple Business Impact Analysis plan for a non-profit I actively volunteer with.



BUSINESS IMPACT ANALYSIS USING STRATEGIES FROM NIST 800-53 AND ISO 20071

In this example, here I walk you through an instance where I use my knowledge of NIST 800-53 and ISO to construct a simple Business Impact Analysis plan for a non-profit I actively volunteer with. The main idea will be to implement an IaaS to provide fault tolerance for it's mission critical process. The VDI is the bread and butter of the organization's core mission.

Process:Virtual Desktop Infrastructure

Operational and Financial Impacts

Timing/Duration	Operational Impacts	Financial Impact	Notes
> 24 Hours	Customer dissatisfaction	High	This can damage your ability to maintain contracts and reputation of the organization
> 8 Hours	Contractual Penalties (Breach of contract)	>150k	Notify all partners about the VDI outages so parents and staff can be prepared, This can damage your ability to maintain funding for the project
> 24 Hours	Delay in stragic initative	Low	It's not too bad, once the VDI is backup, you can continue mission critical proccesses.
< 1 Week	Increased expenses (overtime labor, outsourcing, expediting cost)	Medium	In no uncertain terms this can be tricky. We can outsource the VDI process as IaaS, but this comes this with increased budget.

	Considerations:	For this function, we can keep the same proctol with turning it on and off during seasonal operations, but i'd recommend to purchase some IaaS to use as fault tolerence so we can avoid any complete outages.
	Impact Level Legend:	Low
		Medium
		High

BUSINESS IMPACT ANALYSIS USING STRATEGIES FROM NIST 800-53 AND ISO 20071

In this example, This is a visual of how data backups are created with the companies I work with I construct data backups based on customers needs and mission critical processes.

Object	Approximate size	Business impact of data loss	Recovery time objective (maximum time the recovery process will take)	Recovery point objective (maximum amount of time between backups)	Maintenance window (time available to complete backup)	Backup tool selected	Backup interval (time between backups)	Recovery strategy (how you will recover this object)
[redacted]								
Local Data	10GB	High - In the worst case scenario the department would lose 1 years+ worth of work which would result in mission critical projects being impossible to complete.	1 Hour	0	24 Hours	Google Drive	Bi-Weekly backup via first Monday of each month.	Google Drive

HOME LABS

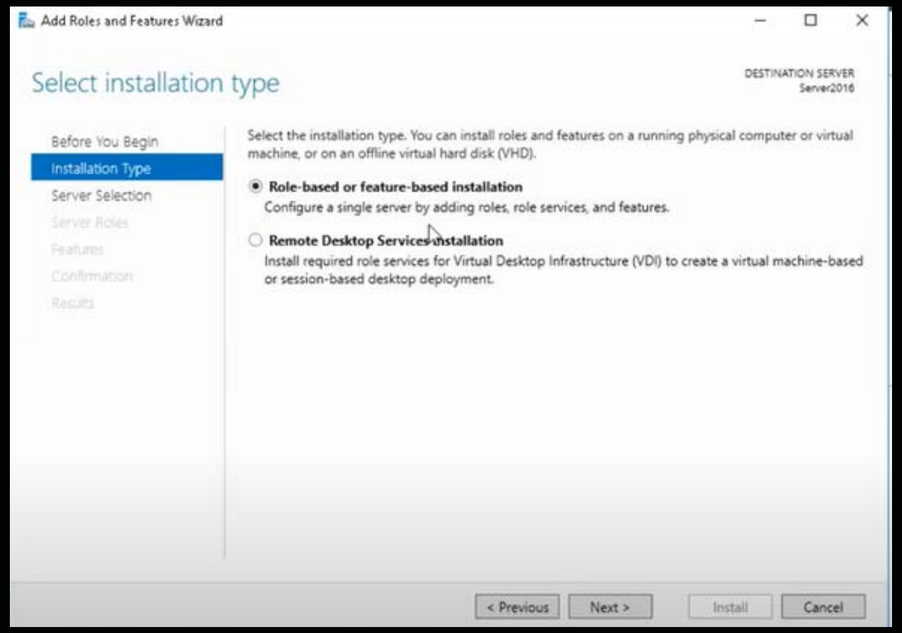
The following are all home labs projects I've worked on in the last two to three years. These labs demonstrate how I take time to practice the fundamentals of basic computing skills and how I've set up my own personal network and servers at home.

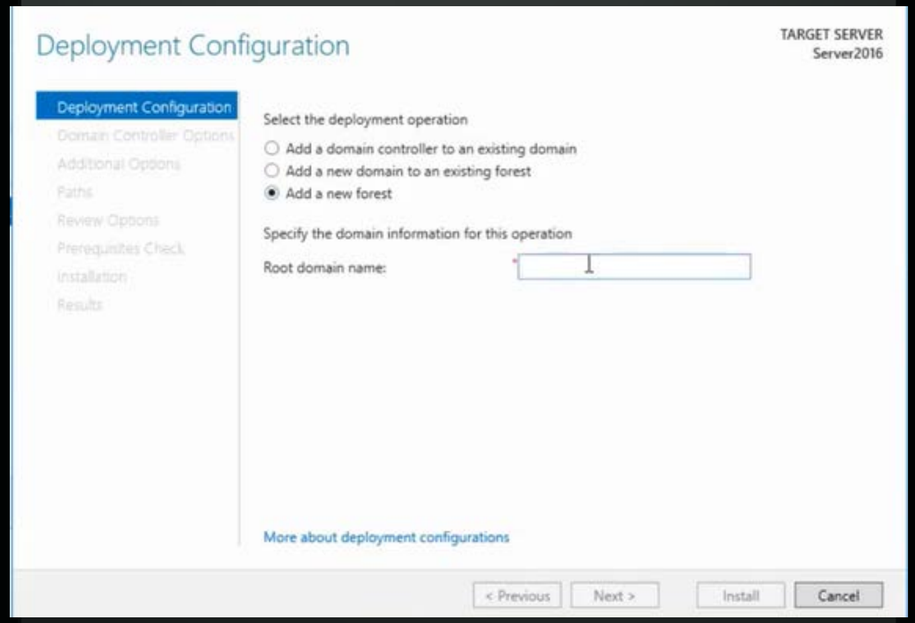
SETTING UP MY OWN AD SERVER.

In this demostration I will walk you through on how I set up my own Virtual Machine using Oracle VM VirtualBox and how I configured my own Microsoft Active Directory Server.

CONFIGURING THE SERVER

Here the first steps to set up my Windows Server was making sure I renamed the machine to Windows Server2026 from the generic computer name. After that I proceed to install Active Directory. I named my server and continued to install all tools.





CYBERSECURITY TRAININGS

The following are all cybersecurity trainings i've have done personally or guided by a certified InfoSec Analyst.

Trainings

Knowbe4 Cyber Security Training: Vulnerabilities and Social Engineering

Knowbe4 Cyber Security Training: Social Engineering Red Flags

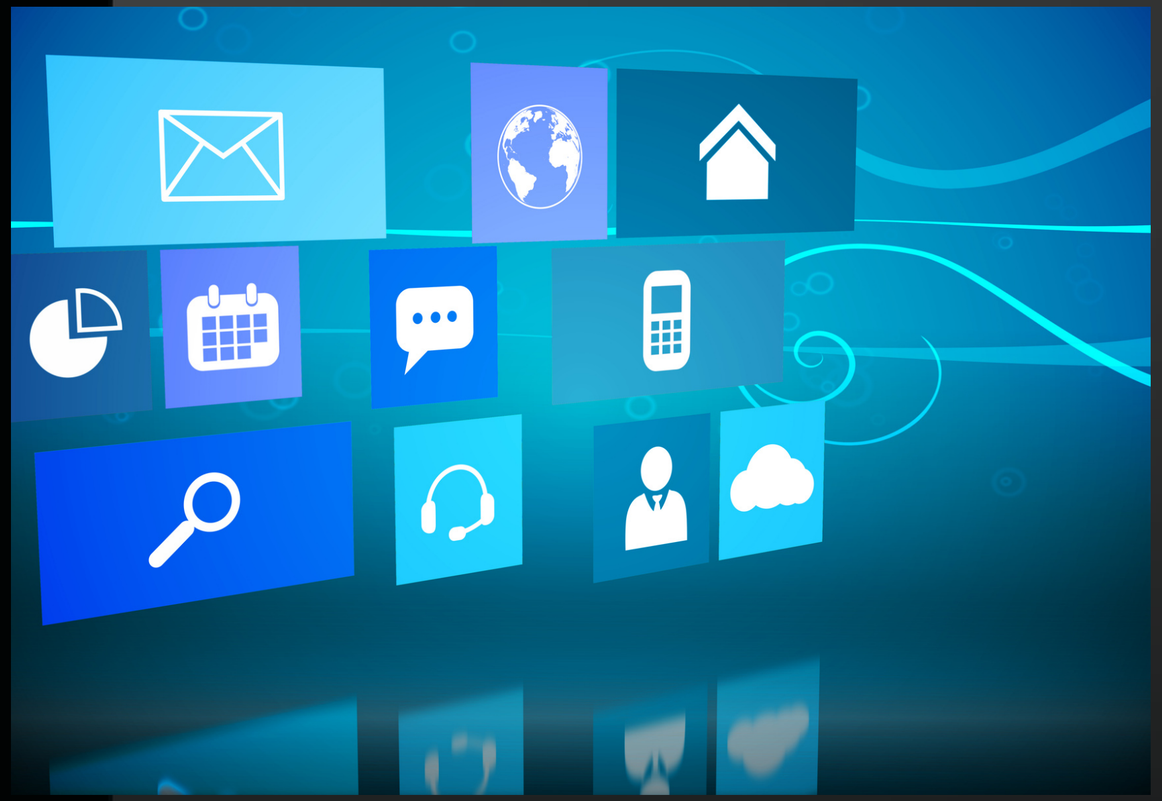
Knowbe4 Cyber Security Training: How to Become a Human Firewall - Defining Human Firewalls

Knowbe4 Cyber Security Training: Creating Strong Passwords Security Awareness Training

Knowb4 Cyber Security Training: Cyber Security Essentials: Secure Data Handling

Knowbe4 Cyber Security Training: Kevin Mitnick Security Awareness Training

MITRE ATT&CK Framework - Cybrary Labs



APPLICATION PORTFOLIO

The following are all computer applications I've configured, troubleshooted and installed on machines.

SentinelOne
Google Chrome
Zoom
Deep Freeze
Fortinet
Microsoft Office
KACE
Outlook
Firefox
LogMeRescue

Leica
CCURE
GMAIL
TeamViewer
LogMeRescue
Smartsheets
Zendesk
LogMeRescue
LibCal
Medicat

Microsoft Active Directory
Adobe Creative Cloud
Cisco Meraki
Aruba Airwave
Canvas
Microsoft LAPS
Dell DDP

COMMUNITY SERVICE & TUTORING

The following are all community service organizations and tutoring sessions I've had within the IT space.

VARSITY TUTORS: COMPTIA A+ AND NETWORK+ TUTORING.

TUTORING COMPTIA A+

In my A+ tutoring sessions, I helped students understand and conceptualize the main domains of CompTIA's A+ certification exams. Without displaying the personal information or the identities of the students I've worked with, I've used some techniques to guide the student onto a proper plan for success.

What are your goals and outcomes for your tutoring sessions?
What do you know already?
Where do you experience the most challenges in this course?
What is your timeline for taking the test?
Have you attempted the test yet?

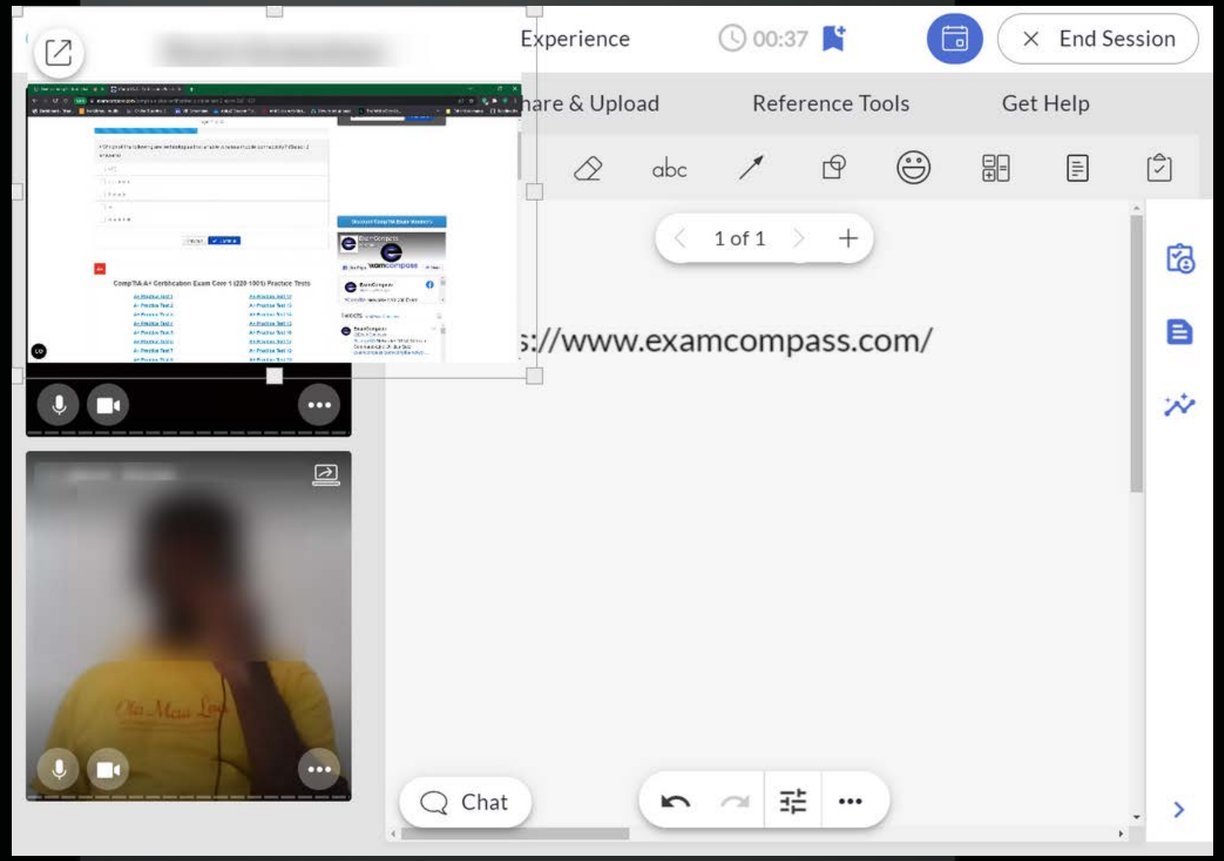
Some strategies for test-taking.
1. Skip past the PBQs and do them last.
2. Use the process of elimination for multiple choice.
3. Flag the questions you don't know and come back to them to save time.

TUTORING COMPTIA A+

In my A+ tutoring sessions, I helped students understand and conceptualize the main domains of CompTIA's A+ certification exams. Without displaying the personal information or the identities of the students I've worked with, I've used some techniques to guide the student onto a proper plan for success.

What are your goals and outcomes for your tutoring sessions?
What do you know already?
Where do you experience the most challenges in this course?
What is your timeline for taking the test?
Have you attempted the test yet?

Some strategies for test-taking.
1. Skip past the PBQs and do them last.
2. Use the process of elimination for multiple choice.
3. Flag the questions you don't know and come back to them to save time.



TUTORING COMPTIA NETWORK+

In my Network+ Tutoring sessions, I've implemented the same strategy with my students. Although it's increasingly more challenging than the A+ exam. I start with teaching the network fundamentals and then network troubleshooting. Understanding the OSI Model and giving my students Memonics to remember it has truly helped them in the long run.

ARTICLES PUBLISHED

Take a look of articles that have been published by me. Feel free to comment and provide critiques.

HOW TO EARN YOUR COMPTIA A+ CERTIFICATION IN 2022.

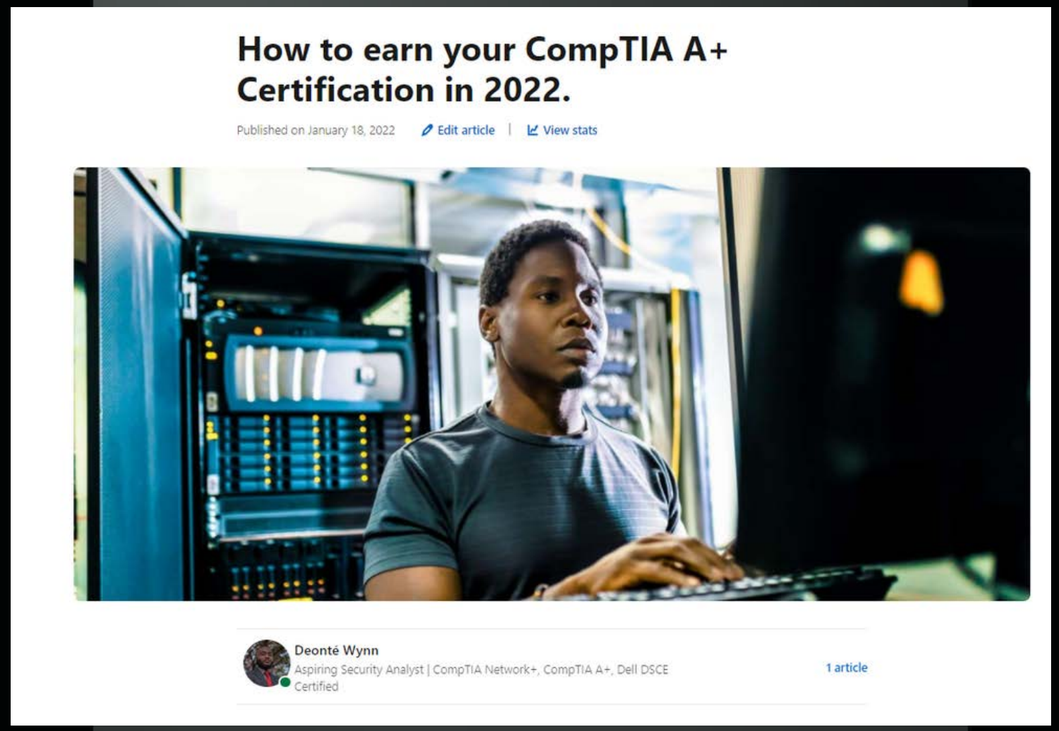
Deonté Wynn
Aspiring Security Analyst | CompTIA Network+, CompTIA A+, Dell DSCE Certified
1 article

Getting your CompTIA A+ Certification can be challenging, not to mention you must pass two separate exams. The exams test your ability on basic computer hardware and software concepts which encompass a wide range of topics. Attaining your CompTIA A+ certification will open new doors for your career in IT, and it is only the beginning. CompTIA formats their exams with 75 or more multiple-choice questions with a few Performance-Based Questions or PBQ's. Depending on the exam, a minimum score is required to pass.

When preparing for the exam it's important to fully understand the concepts before actually taking the test. I suggest that one taking the exam study at least a minimum of two months to understand the material. After you've read and understood a good percentage of the material, review and go over your notes.

Once you feel confident, I'd take a couple of practice exams before you attempt the actual test. Completing a few practice exams will train your brain to be exam-ready. Understanding and memorizing key concepts will help you succeed come exam day. You want to train for the exam like how an athlete would train for a championship game. This means you must have a dedicated schedule, you must go over weak points in your game, you need to put in overtime for studying, and most of all you need to be CONSISTENT.

One must complete two exams to pass and become A+ certified. The exam objectives are listed as follows.



CONFERENCES ATTENDED

All of the following are conflerences attended in the indusry

SANS NEW2CYBER SUMMIT 2022

SANS NEW2CYBER Summit is aan informational conference giving atendees practical steps to get into cybersecurity. Professionals from all over share knowledge and insight on industy trends. It was a great conference. Lots of connections were made!

REFERENCES

Damian Simmons - AVP (Assistant Vice President) End-User Computing (EUC)
SiriusPoint Ltd., Hamilton, Bermuda

Please request for more references, if needed.

THANK YOU

I appreciate your undivided attention. Please feel free to contact me via phone or LinkedIN. I have hoped you enjoyed my IT Demo.

Telephone
484-343-6010

LinkedIN
Deonte Wynn

Email
dwynn93@gmail.com